



**Carnegie Mellon
Software Engineering Institute**

Pittsburgh, PA 15213-3890

Maturing Your Approach to “Security Management”

Richard A Caralli, William R Wilson
Survivable Enterprise Management Team

Networked Systems Survivability
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Sponsored by the U.S. Department of Defense
© 2004 by Carnegie Mellon University

Report Documentation Page			<i>Form Approved OMB No. 0704-0188</i>	
<p>Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p>				
1. REPORT DATE JAN 2004	2. REPORT TYPE	3. DATES COVERED 00-00-2004 to 00-00-2004		
4. TITLE AND SUBTITLE Maturing Your Approach to 'Security Management'		5a. CONTRACT NUMBER		
		5b. GRANT NUMBER		
		5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S)		5d. PROJECT NUMBER		
		5e. TASK NUMBER		
		5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Carnege Mellon University, Software Engineering Institute, Pittsburgh, PA, 15213		8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)		
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited				
13. SUPPLEMENTARY NOTES				
14. ABSTRACT				
15. SUBJECT TERMS				
16. SECURITY CLASSIFICATION OF:		17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified	25	



Key topics

Challenges for doing “security”

Security approach roadblocks

New perspectives on the problem

Maturing your security approach



Organizational challenges -1

Scope of security is the entire organization

Requires management and technologists to work together

Industry bias toward technology solutions

Forces constant risk vs. reward trade-offs

Not naturally a profit-centric activity





Organizational challenges -2

Not a core competency of an organization

Requires everyone in the organization to play a part

Everyone has a different view and objective

Lack of common language and lexicon

Lack of data and metrics





Why do we fail?

There are several natural barriers to effectiveness

May be unlike any problem organizations have had to solve (somewhat resembles Y2K)

Complex problem requires an adaptive, flexible approach



Common problems

Defining the wrong target

Focusing too narrowly

Treating security as a technical specialty

Managing to regulations

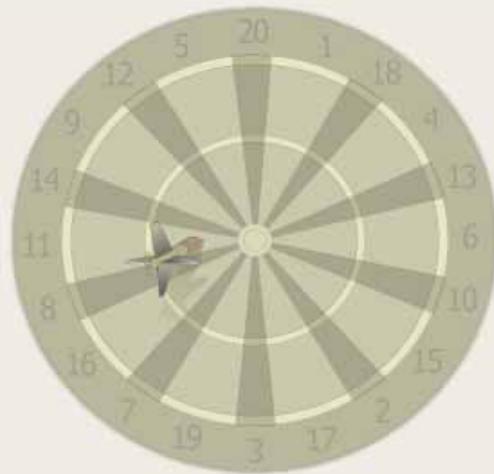
Failure to recognize complexity



Defining the wrong target

Problem

The desired outcome of the security approach is ambiguous.



Symptoms

Unclear security goals

Goals not well communicated

No measures for success

Can't assure stakeholders that "security" has been accomplished



Narrow focus

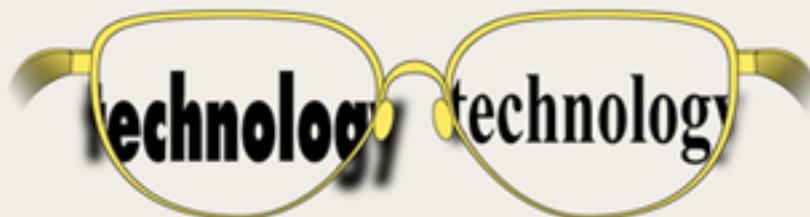
Problem

Focus of security approach
technology-centric

Symptoms

Security viewed as a
technology problem

Assumption that secure
technology = secure
organization

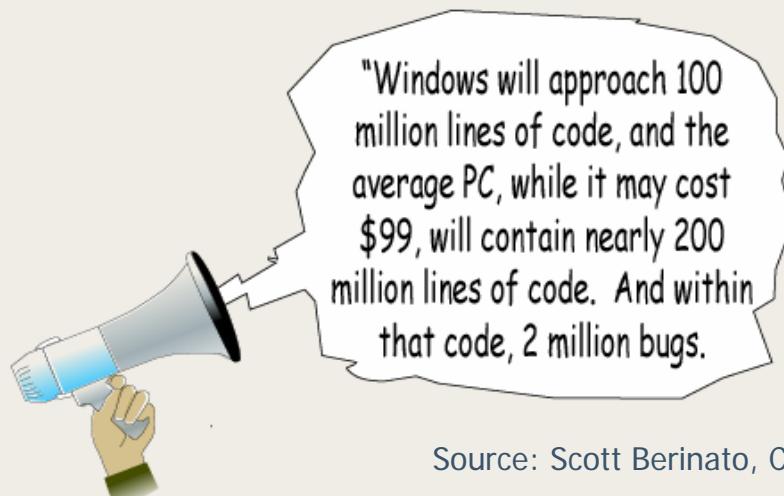




Technical specialty

Problem

Implementation and monitoring of security approach is a technical specialty.



"Windows will approach 100 million lines of code, and the average PC, while it may cost \$99, will contain nearly 200 million lines of code. And within that code, 2 million bugs.

Symptoms

CSO/CISO and security professionals in technical roles

IT is exclusive domain of security activities

IT owns security approach or strategy

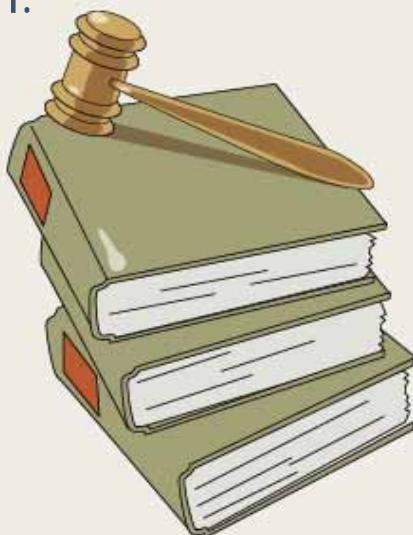
Source: Scott Berinato, CIO Magazine, December 15, 2003



Regulation-driven

Problem

Regulatory compliance defines the purpose and direction of the security approach.



Symptoms

Regulations overly influence the approach

Comply with regulations = secure organization

Security standards derived from regulations



Lack of flexibility

Problem

The security approach cannot adapt to changing environmental conditions.



"The chief security officer should now be positioned as a trusted advisor to the business, moving away from operational delivery towards understanding and managing risk."

Symptoms

Security approach quickly obsolete

Approach out of sync with organization's strategic objectives

Time spent on securing assets that are not critical to accomplishing the mission

Source: Miya Knight, www.vnunet.com/news/1147007



Organizational impacts

Misalignment of operational and security goals

False sense of accomplishment

Failure to utilize all necessary skills/resources

Compliance at the expense of effectiveness

Approach breaks at every twist and turn

Overall ability to manage security is impaired



Maturing your approach



Change your perspective

Expand your objective

Let the organization drive

Embrace the resiliency concept

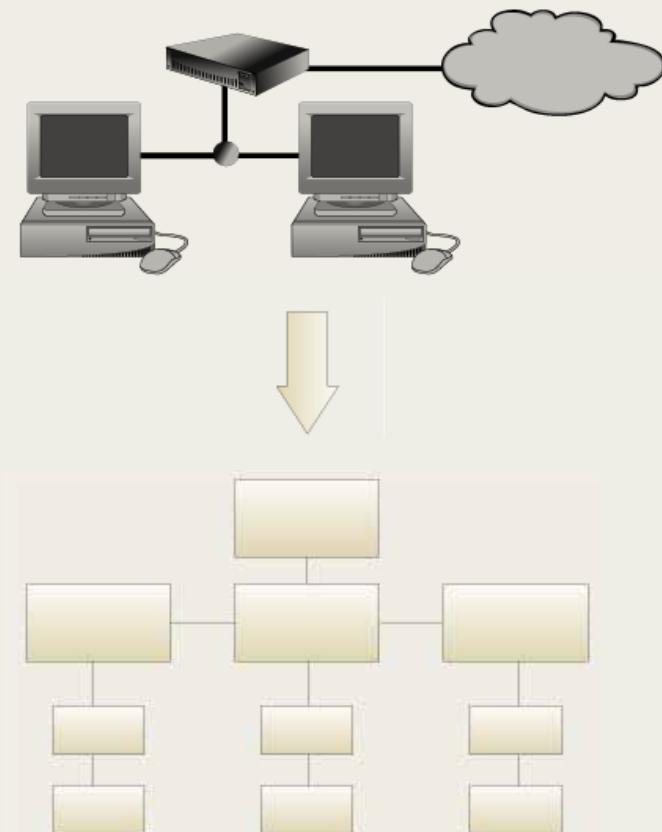


Expand your objective

View the organization as the benefactor of “security” not IT

Change perspective from **technical** “network” to **organizational** “network”

Aim to make the organization’s mission both **sustainable** and **adaptable** to its environment





Let the organization drive

Use organizational drivers—mission, strategic objectives, goals, CSFs—as the foundation for security

Align security strategy and approach with drivers and ensure they are adaptable to changes

Aim for sponsorship as high in the organization as possible



Move from security to resiliency





What is resiliency?

Physical property of a material that allows it to spring back after deformation that has not exceeded its elastic limit [www.cogsci.princeton.edu]

“. . .ability to withstand systemic discontinuities”
[Booz Allen]

“. . .ability to adapt to new risk environments”
[Booz Allen]

Source: Booz Allen - Enterprise Resilience: Managing Risk in the Networked Economy



Security vs. resiliency

Security

Asset-focused



Reactive

Protective (defensive posture)

Maintain and sustain

Active

Resiliency

Organization-focused



Proactive

Adaptive (offensive posture)

Sustain *and improve*

Transparent



Resilient organizations

Align capabilities to collaborate

Elevate risk management to organizational level

Rely on the system of internal controls

Sense, respond, and improve

Establish transparency



Moving toward resiliency -1

Sharpen the target

Utilize critical success factors for alignment

Utilize and mobilize the capabilities of the organization

Involve the right people—spread responsibility throughout organization



Moving toward resiliency -2

Rely on operational excellence

Rely on strong system of internal controls

Manage as a process and improve

Select metrics for success and measure!



**Carnegie Mellon
Software Engineering Institute**

Questions?



For more information

Networked Systems Survivability Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213 USA

www.sei.cmu.edu
www.cert.org

Rich Caralli
rcaralli@sei.cmu.edu



Presentation references

Randy Staff, Jim Newfrock, and Michael Delurey, "Enterprise Resilience: Managing Risk in the Networked Economy," *Enterprise Resilience: Risk and Security in the Networked World*, 2003 Booz Allen Hamilton; www.strategy-business.com

Scott Berinato, "The Future of Security - After the Storm, Reform," *CIO Magazine*, December 15, 2003; www.cio.com/archive/121503/securityfuture.html

Miya Knights, "Process not technology tightens security," (quoting Phillip Gregory of Norwich Union) March 11, 2003; www.vnunet.com/news/1147007